Office of Information Technology Services

Strategic Plan for Information Security 2007

Overview:

This strategic plan sets the goals and objectives of the state in the operation of its business systems related to the protection of the state's information. Today, many of the State's most critical business systems are automated. Therefore it is important to translate the business needs of the state into a strategic technology plan that details how information technology (IT) contributes to achieving the goals of providing secure services to citizens. This plan supports the State CIO's strategic planning initiatives including, IT consolidation, Information Technology Infrastructure Library (ITIL) and asset management. The means to achieving the level of information protection driven by the business needs is supported by policies, standards, procedures (PSPs) and the technical architecture. The PSPs are the rules for operating and protecting the information. The technical architecture is the technology that is used to implement the strategic plan. Information security measures need to be woven into the fabric of IT operations.

Listed below are the strategic information security goals:

1. Manage risk to improve agency security posture through consolidation of IT infrastructure.
2. Improve security processes by incorporating Information Technology Infrastructure Library (ITIL) process methodologies into security operations.
3. Combat security vulnerabilities with an enterprise approach to vulnerability management.
4. Enhance cyber incident response capabilities by expanding preventive activities and forensic services.
5. Protect the confidentiality, integrity and availability of the State's IT information by defining and implementing a consistent approach that meets legal and regulatory requirements relating to confidential and/or personally identifiable information (PII).
6. Support efforts to simplify and standardize identity management for state employees, vendors and citizens.
7. Enhance the State Information Security Manual framework based on the ISO17799 Standard Toolkit.

These goals are implemented in part through the deployment of information technology. Below each strategic goal is supported by the approach to achieve that goal. In order to achieve these goals in an effective and efficient manner one or more initiatives may need to be defined to select and optimally deploy information security solutions.

Strategic Goal
#1. Manage risk to improve agency security posture through consolidation of agency IT infrastructure.

Summary:

The State has a responsibility to develop, deploy, and manage business systems that contain the appropriate security controls to protect citizen information in an effective and efficient manner. Security controls need to be included in all aspects of the systems development and operational life cycle, including planning for system retirement. Agency business systems benefit from using a robust infrastructure with a layered approach to security controls, monitoring, metrics and reporting. As a system is put into operation the system security controls need to be monitored and tracked to ensure that they do not become obsolete or inadequate due to changing requirements.

Implementation Approach

- Reduce agency responsibility for operating and securing infrastructure
- Review agency applications and project plans to ensure that they include adequate and appropriate security mechanisms.
- Implement risk based approach to secure enterprise hosting environment that includes security controls.
- Encourage and support agency efforts for securing their applications.
- Support implementation of infrastructure security controls (ESAP, risk assessment and framework placement, patch and vulnerability management, scans, IDS/IPS etc).
- Monitor and report on the effectiveness of security controls.
- Integrate agency consolidated operations with ITS cyber incident response plans.

Office of Information Technology Services

Strategic Plan for Information Security 2007

Strategic Goal
#2. Improve security processes by incorporating Information Technology Infrastructure Library (ITIL) process methodologies into security operations.

Summary:
The State has a responsibility to maintain the operational availability, confidentiality, and integrity of information processed by systems. ITIL, the *de facto standard* used in the IT industry encompasses the foundation for IT Service Management (ITSM). ITIL is a transformative process built on best practices or recommendations that implement a shift from a strict focus on technology to a focus on delivering highly available services. Spanning the entire ITIL framework are the essential security controls necessary to ensure availability of services while protecting citizen and employee information in an effective and efficient manner. ITS business systems benefit from using a standardized methodology that has imbedded within its core functionality a layered approach to security controls, monitoring, metrics and reporting.

Implementation Approach

- Provide detailed, ongoing support by participating in teams developing, implementing and managing the elements of Service Support and Service Delivery.
- Convert the internal security processes to an ITIL framework based on regulatory requirements, State standards and policies, best practices and practical experience in operating security in a State agency.
- Ensure the six security measures as defined within the ITIL framework – preventative, detection, reductive, repressive, corrective and evaluation – are properly defined in the implementation build out and daily operation.
- Monitor Critical Success Factors (CSFs) with developed Key Performance Indicators (KPIs) to achieve and maintain confidentiality, integrity and availability values.
- Ensure Operational Level Agreements (OLAs) and Service Level Agreements (SLAs) are defined, negotiated and maintained to support key security services.
- Define and implement evaluation processes to verify compliance, to respond to inappropriate use and to measure the effectiveness of security measures.

Strategic Goal
#3. Combat security vulnerabilities with an enterprise approach to vulnerability management.

Summary:
The State has a responsibility to develop, deploy, and manage Information Technology services in a cost effective and efficient manner. Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. Proactively managing vulnerabilities of services will reduce or eliminate the potential for exploitation and the costly impact of time and money spent recovering from exploitation. Industry best practices recommend that all organizations have a systematic, accountable, and documented process for managing exposure to vulnerabilities.

Implementation Approach

- Define, procure and operate an efficient, effective Vulnerability Management system that incorporates the latest concepts and methodologies for enhanced, in-depth layered security.
- Establish quantifiable, results-oriented metrics customized to provide each stakeholder a view of their security performance.
- Enhance vulnerability remediation through network, host and application scanning providing information to administrators that has been screened and prioritized by critical needs.
- Monitor security sources for vulnerability announcements, remediation and emerging threats.

- Establish and maintain a database of vulnerabilities and actions taken to mitigate and/or remediate.
- Support asset and configuration management initiatives in order to integrate the inventory of ITS resources to determine which hardware equipment, operating systems, and software applications are used by the organization with the vulnerability management process.

Strategic Goal
#4. Enhance cyber incident response capabilities by expanding preventive activities and forensic services.

Summary:

The state has a responsibility to effectively respond to cyber security incidents. Additionally the state has a responsibility to take a proactive approach to preventing cyber security incidents. The ability to disseminate timely warnings to constituent agencies and other ITS customers is paramount in this effort. Providing a centralized source for this information ensures consistency and eliminates the need for duplicated efforts across state government. When a cyber security incident occurs or misuse of state network and computer resources takes place, the ability to investigate the root cause and collect evidence is an essential part of cyber security incident response. In many cases the collection and preservation of evidence is necessary to meet legal and regulatory requirements and/or agency policy. Establishing a dedicated forensics lab with qualified staff to provide this service ensures the state is utilizing trained staff to follow standard evidence collection practices. The evidence gathered in this manner may be used in various legal proceedings or released to the appropriate law enforcement authorities without a subsequent need for the evidence to be re-processed.

Implementation Approach

- Maintain up to date incident management plan.
- Review agency incident management plans.
- Act as State of North Carolina representative to the Multi-State Information Sharing and Analysis Center (MS-ISAC).
- Provide timely updates on new cyber security threats through e-mail notifications, security web portal, and other means as required to protect the state's network and computer resources.
- Augment existing Security Web Portal with interface to dedicated US-CERT portal for North Carolina.
- Provide yearly incident management training to constituent agencies and customers.
- Develop a standard rate for forensic services.
- Provide computer forensic services to state agencies.
- Maintain a database of cyber security incidents when reported or detected.
- Provide statistical information and monthly reports to ITS management, the State Auditor and North Carolina Attorney General.
- Provide security consulting services to agencies in regard to provided services.

Strategic Goal
#5. Protect the confidentiality, integrity and availability of the State's IT information by defining and implementing a consistent approach that meets legal and regulatory requirements relating to confidential and/or personally identifiable information (PII).

Summary:

There are many legal and regulatory requirements for handling information that is classified by law as confidential and/or personally identifiable information, (PII). Security breaches involving such data often contain requirements for disclosure and/or penalties. Effective October 1, 2006 state agencies must disclose security breaches when PII

is involved. Executive branch agencies must report security breaches to the Enterprise Security and Risk Managment Office. It is important that agencies understand and are prepared to meet these requirements.

Implementation Approach

- Update both the state and the ITS agency cyber incident plan to include PII requirements.
- Update the cyber incident reporting form, database and templates to include PII requirements.
- Work with the portfolio and asset management teams to provide data elements for noting confidential and/or PII data.
- Raise agency awareness through training.
- Identify ITS critical systems with confidential/PII data and update in the ITS incident management plan
- Define communications protocols for confidential/PII data.
- Remind agencies when reporting a cyber incident that they need to take appropriate actions if confidential/PII data is involved.

Strategic Goal
#6. Support efforts to simplify and standardize identity management for state employees, vendors and citizens

Summary:
The state must consistently identify who has access to state IT resources, authentication, and what they can do once they have such access, authorization. Strong identity management mechanisms are a foundational element of information security. Legal and regulatory requirements increasingly require strong forms of identity management. Users of identity management systems need to a have a consistent means of interfacing with state resources through simplified sign on processes that minimizes user confusion while simultaneously enforcing the application of strong and consistent policies and procedures. User access needs to be defined based on their roles in the business process. The business of the state must expand from state employees to service citizens and vendors for critical business functions that require strong identification and authorization.

Implementation Approach

- Support an enterprise approach to identity management though the NCID service offering.
- Define and update state and ITS agency PSPs related to identity management.
- Support efforts to integrate various platforms with enterprise identity management service offerings, including but not limited to badge system, RACF, wireless networks, etc.
- Support implementation of dual factor authentication (begin with systems and database administrators) by integrating use of certificates, tokens, smartcards, biometrics, etc.
- Support state efforts to understand and comply with federal REALID requirements.
- Monitor and report on compliance with legal and regulatory requirements.
- Review agency project plans for appropriate identity management approach.
- Engage the Technology Planning Group (TPG) and agency staff in the identity management process.

Strategic Goal
#7. Enhance State Information Security Manual Framework Based on the ISO17799 Standard Toolkit

Summary:
The State needs to continue to build upon its current foundation to continually enhance the State Security Policy, Standard and Procedures and Architectural (PSP) framework. Agencies need help in identifying gaps and tailoring their

agency policies within the State framework to meet their own unique requirements. In this way the State can ensure that all agencies have a common baseline of PSPs integrated with the state level framework.

Implementation Approach

- Provide support to agencies through an enterprise license for the ISO17799 security standard and toolkit.
- Train agencies on ISO17799 and the state security manual.
- Engage the TPG and agency staff in the security manual review process.
- Perform security standards gap analysis.
- Provide for regular updates to the security manual content.
- Follow process established by the State CIO related to enterprise standards.
- Evaluate agency IT projects for compliance with PSPs.
- Assess agency PSP compliance, monitor and track deviations.
- Encourage agencies to complete agency PSPs.